Criminogenic qualities of the Internet

Max Taylor

To cite this article: Max Taylor (2015) Criminogenic qualities of the Internet, Dynamics of Asymmetric Conflict, 8:2, 97-106, DOI: 10.1080/17467586.2015.1065082

To link to this article: http://dx.doi.org/10.1080/17467586.2015.1065082

Published online: 12 Sep 2015.
Criminogenic qualities of the Internet

Max Taylor*

Department of Security and Crime Sciences, University College, London, UK

This paper initially identifies a number of critical distinctions that might help our understanding of the relationship between Internet use and terrorism. It then develops the notion of complex global microstructures as a useful conceptual aid to understanding how people interact with the Internet in general, and to terrorism in particular. Parallels are identified between various inappropriate, risky and dangerous uses of the Internet which are argued to point to a degree of commonality of effect. The paper concludes by suggesting that some forms of user interaction with the Internet suggest the Internet may have criminogenic qualities.

Keywords: Internet; criminogenic; microstructures; affordance; morphogenesis

One of the problems in analysing future responses to managing the relationship between terrorism and more generally criminal activity and the Internet is to distinguish between factors that are individual to the potential perpetrator, those that relate to the social context in which problematic activity takes place and those factors that relate to the rapidly changing medium itself (i.e. the Internet). This is of practical significance, in that in the absence of a firm understanding of the relative effect of these factors, initiatives that are wrongly applied are likely to be wasteful if not counterproductive. One complicating issue, however, is that all three factors in themselves and in interaction imply complex and dynamic processes rather than linear causal accounts. A further issue is that it is likely that influences on one are not necessarily equally influential on others. In a sense this is an extension of the critical observation made by Clarke and Felson (1993) distinguishing between “involvement” and “event” decisions in criminal behaviour. Involvement decisions in Clark and Felson’s terms refer to processes through which individuals choose to become involved in criminal activities in general, in contrast to event decisions that relate to the commission of a particular crime. What is critical in this distinction is that the factors that might determine criminal event decisions are very likely to be different from those that concern involvement decisions. When applied to the issues of concern here, whilst perpetrator decisions may reflect interactions of both “involvement” and “event” decisions, as indeed may social context, issues related to the medium itself may be more heavily influenced by “event” decisions. These may be critical distinctions to make, and exploring this further may be of value in the development of more effective policing and preventative strategies.

Taylor and Quayle (2008) and Quayle and Taylor (2015) have suggested that there are qualities of the Internet either in association with facilitating conditions (personal or environmental) or otherwise that in themselves made accessing abuse images of children more likely and in essence operate as “event” factors. Their argument was framed within an analysis drawing on a situational crime control model, emphasizing the significance of
pre-criminal situations and opportunity (Taylor & Quayle 2006). In this short paper, I want to explore further how we might conceptualize these Internet qualities in complex criminal networks, as elements of the “medium” related factors identified above, and subsequently extend that analysis using terrorism as an example. For the purposes of this paper, the complex individual qualities of different Internet platforms are largely ignored, although in a more fine-grained analysis this clearly will be very relevant.

As our understanding of the Internet gradually developed, a number of sources of vulnerability became apparent. These have become known as the 3 As of Internet vulnerability (Cooper, 2000, 2002) – anonymity, affordability and accessibility. More recently other vulnerabilities have been suggested, in some cases even extending it to seven factors (Hertlein & Stevenson, 2010) including approximation to the real world (Ross & Kauth, 2002), enhanced acceptability online of “real world” unacceptable activity (King, 1999), moral and criminal ambiguity (Hertlein & Stevenson, 2010) and accommodation between real and online self (Hertlein & Stevenson, 2010). A structural feature of the Internet that interacts with these vulnerabilities is its essentially non-hierarchical quality. Whilst access to, hosting and searching of services is mediated by commercial and government Internet Service Agencies, the nature of the Internet means that content as opposed to structure is essentially dependent on user activity; furthermore, that content is distributed and that distributed quality is largely characterized by microstructure and self-organization. At the core of the potential future this way of thinking implies lies what might be described as emergence qualities of Complex Global Microstructures (Knorr-Cetina, 2005).

In what follows I would like to explore the concept of Complex Global Microstructures further, because I believe a better understanding of the implications of this offer us a way of moving our thinking forward into different ways of conceptualizing the development of terrorism, and more generally crime, criminal opportunity and activity on the Internet, drawing on ecologically grounded concepts like affordance.1 Knorr-Cetina’s (2005) work has its origins in analyses of the workings of the global financial systems. But it has been used to explore how contemporary terrorist organizations have emerged and may develop in the future, with implications that reach far into other areas of criminal activity.

She notes an important contemporary paradox which may well characterize future criminal engagement with the Internet: the capacity shown by marginal groups (of specific conspirators in the case of terrorists or child pornographers, but of financial traders in the financial world, or of people engaged in broader organized transnational criminal activity) to generate serious threat and undertake complex action, but who are themselves also fragile, dependent on a few key figures, and who make mistakes. Amongst other things, this illustrates in the modern world what seem to be serious disproportionalities between cause and effect, resulting in unpredictable outcomes. This is because although the aggregate of people concerned are themselves weak, and are geographically distributed, they paradoxically show strong self-organizing and highly effective emergent structures. Knorr-Cetina suggests that this illustrates a contemporary example of Complexity Theory (Kauffman, 1997), emphasizing microstructure and emergent adaptive mechanisms of coordination, in what MacLennan (2007) has referred to as the emergent phenomena of complex systems. The emergent processes we are referring to may be conceptually very closely related to ideas introduced by Turing (1952) in his notions of Chemical Morphogenesis. Turing showed how non-linear partial differential equations could describe and explain the development of an initially homogeneous mixture of chemicals into the asymmetrical forms seen in biological structures. Although largely ignored when
initially made, these observations are potentially very significant, and suggest there may be fundamental parallels to be drawn here in terms of adaptive processes with the physical as well as biological sciences.

In an ecological sense, a complex system is made up of a large number of relatively simple elements, interacting with each other (an example of which is the Internet), such that the emergent behaviour of the whole is difficult to predict from the behaviour of the parts. A quality of complex systems of this kind is that they can be highly adaptive and respond to environmental change in ways that maintain or even improve their functions. If we think of this in evolutionary terms, this adaptive process therefore represents a very effective survival strategy resulting in a system remaining organized and developing in changing circumstances. Where this adaptation is expressed in terms of illegal activity, this represents an enormous challenge to regulatory and law enforcement agencies. Of course, the same processes can also result in maladaptive adaptation, in which case presumably the organism or social structure fails to survive and collapses and dies, or changes again.

Although there may be uncertainties around understanding the detail of these processes, for our purposes, the emergent properties that such systems show cannot be explained by simple linear interactions between elements or components of the system. One powerful example of this is the capacity in complex systems to amplify random fluctuations that result from positive feedback within a system; processes like this lie at the core of Turing’s early analysis of biological change. “Such a system, although it may originally be quite homogeneous, may later develop a pattern or structure due to an instability of the homogeneous equilibrium, which is triggered off by random disturbances” (Turing, 1952, p. 5).

In practice, this process may be a highly adaptive mechanism, because it can break symmetries and balances of forces that might result in blocking change. The paradox of Buridan’s Ass is an example of how (even in antiquity) the challenge to decision making of behavioural symmetries and balance was recognized as a fundamental issue. The paradox of Burridan’s Ass describes an Ass that is equally hungry and thirsty being placed equidistant from food and water. If we assume choice in this setting relates to closeness, the Ass as a rational actor cannot make a rational decision to choose one over the other, but will be influenced by random and unsystematic changes. Parallels between this paradox and the actual behaviour of digital logic gates can be made. The critical practical point here is that despite the abstract quality of this discussion, understanding the feedback mechanisms involved in real-life situations that illustrate this problem may show means for eliminating or weakening them, and identifying potential new structures.

We can also sometimes see in complex social systems what have been referred to as “phase changes”, or tipping points, where rapid change results from relatively minor changes or fluctuations in conditions within or from outside the system. I wonder, for example, if this is how we should think about the “Arab Spring” — in this sense a local social fluctuation (which it is important to stress can occur without any necessary contemporary ideological or political cause) amplified through positive feedback through the digital technologies (such as social networks) results in unpredictable and long-lasting (and largely unpredictable in the short term) change. The direction of change, however, may not necessarily be uniform and may equally be unpredictable. Such phase changes may underlie emergent qualities (Paperin, Green, & Sadedin, 2011), who suggest that “recurrent phase changes in the interaction density of system components (i.e. density of underlying interaction networks) constitute a general mechanism for self-organization in biological complex adaptive systems (CAS), as well as in some non-living complex systems” (p. 609).
Complexity theory (Kauffman, 1997) suggests that such sudden rapid changes are qualities of complex systems, and this has been used not simply to explain micro changes to behaviour, but also big changes, such as the rapid decline of the British Empire (Fergusen, 2010).

Because contemporary examples of such changes are on-going, the long-term adaptive qualities (and therefore survival) of these changes really remain to be seen; but the process seems clear enough. The adaptive selection processes may be what we describe as self-organization, but it does not necessarily imply some kind of teleological awareness, and what we see is in effect simply the operation of adaptive evolutionary processes. They illustrate the positive value of error, uncertainty, noise, variability and other kinds of simple variation. These mechanisms, however, do not necessarily have to work perfectly to be effective, nor do they lend themselves to linear modelling – indeed they illustrate the productive value of error and unpredictability, as selection eliminates unproductive avenues. Imperfect exploration of options (even if guided by affordance qualities) paradoxically results in positive unbiased exploration, macroscopic reorganization and enhanced adaptation. The counterintuitive quality of valuing variability and unpredictability therefore has adaptive value by limiting local, temporal or immediate bias. In essence, what we are describing here might also be illustrated in work on artificial neural networks, where rule-like behaviour can be generated without actually having explicit system rules. As with affordance, the rule-like quality essentially lies not in the observer, but the actor.

What we might describe as elements of a new global terrorism and criminality illustrate an emergence of global microstructures of this kind, reflected in “forms of interconnectivity and coordination that combine global reach with microstructural mechanisms that instantiate self-organising principles and patterns” (Knorr-Cetina 2005). A basic quality is that such global microstructures are essentially communities of practice (Wenger, 1998) linking up and stretching across time zones. However, their emergent properties need not imply increased socio-institutional complexity; indeed, as Knorr-Cetina notes, paradoxically they may become feasible only if they avoid complex institutional structures. In a topical and very prescient way she draws analogies with how global financial markets work. She suggests that such global markets based on microstructural principles do not exhibit institutional complexity but rather illustrate asymmetries, unpredictability and even the playfulness of complex (and dispersed) interaction patterns. In a challenging statement she suggests that

order is not the outcome of purified social processes and is always intertwined in chaos … these systems manifest an observational and temporal dynamics that is fundamental to their connectivity, auto-effective principles of self-motivation, forms of outsourcing, and principles of content that substitute for the principles and mechanisms of the modern, complex organization. (Knorr-Cetina, 2005, p. 214)

Knorr-Cetina identifies four characteristics of global microstructures that are relevant to our understanding of complex criminal networks:

(1) They are institutionally “light”. The central elements are not those associated with formal authority, complex hierarchies, rationalized procedure or deep institutional structures. They are more like face-to-face structures, but importantly hold across distances.

(2) They exhibit non-Weberian effectiveness. They are not highly rationalized, but nevertheless are effective – and the effectiveness is essentially dependent on systems of amplification and augmentation. As such they exploit disproportion-
alities between input and output, effort and effect, and in so doing illustrate adaptation that is grounded in a local context but meeting global needs.

(3) They cannot simply be reduced to networks. They may comprise a variety of relational arrangements, but they are not in this sense sparse social structures. Their “relational arrangements” are not just concerned with passage of information, but are dependent on (and shaped by) culture, religion, family – with reference to this she draws attention to role of “scopic media”.

(4) Complex global microstructures exhibit temporal as well as physical complexity.

As we have noted above, unstable components increase complexity and thereby paradoxically contribute to stability, because non-enduring components change in response to the irritations of an always more complex environment, and help the larger system cope with external factors. As part of this process, continual disintegration and change creates space for successor elements that increase complexity and the chance of survival. These changing patterns of relatedness factor in success of reproduction of system (which suggests emergent qualities might characterize these systems). As Knorr-Cetina (2005) notes with respect to terrorism, but which may well characterize other criminal conspiracies of this kind, the “lived time of the terrorist appears ‘transcendent’ in regard to personal life, and transcends ordinary time by ‘shadowing’ it with a second future that embeds everyday activities within a new meaning structure” (p. 219).

Castells (2000) has written extensively about the potential for social change of the Internet, including the changes in social structures such as distinctions between private and public space, personal and global communication, and self-defined as opposed to organizational fulfilment of need (illustrated in a trivial sense by the changes in music consumption, and less trivially in public discussion, debate and access to power). Knorr-Cetina has extended these ideas further, however, by embracing temporal qualities – what is referred to as “sequentialization”, where a sense of location in both time and space cease to be of significance. This analysis has profound potential consequences, in that, as noted earlier, it challenges Weberian assumptions of organization and order. In Knorr-Cetina’s words, “the texture of the global world becomes articulated through microstructural patterns that develop in the shadow of (but liberated from) national and local institutional patterns” (Knorr-Cetina, 2005, p. 215).

The significance of microstructures in new terrorism

We can explore this further with respect to the criminal activity we refer to as terrorism. First of all it is necessary to distinguish between “new” and “old” forms of terrorism. In the sense used here and contrary to most usages, the critical element in this distinction is the role of contemporary media as a facilitating factor. “Old” terrorism (the term as used here refers to how it is generated, not age or history – there may be new “old” terrorist groups emerging) does not necessarily depend on contemporary media sustenance. Given a general sense of personal motivation (perhaps related to grievance, perhaps to social awareness and context, perhaps related to peer or kin pressure), the Provisional IRA and the Rote Army Faktion, as examples of “old” terrorism, gained strength from a wide array of personal and contextual factors, such as some sense of culture, history and ideology. Given the same sense of personal motivation. “New” terrorism in contrast depends on and is essentially a part of the new digital media (although expressed in the offline world). Digital (and print) media is clearly a necessary element to understanding old terrorism, but for new terrorism digital (and especially visual) media is a sufficient, rather than necessary condition for
understanding. There are clear parallels to be drawn here with other forms of Internet-based complex criminal conspiracies not primarily based on money, notably the trade in and collection of abuse images of children. Scopic qualities may be of particular significance, with parallels in this sense to be drawn with the beheading and murder videos.

The distinction between old and new might not be conveniently binary, however, and it seems to me likely that individuals (or aggregations however expressed) might well move between old and new forms, and it may well be that the factors that facilitate such transition are an important quality in judging risk. Contemporary foreign fighters (as distinct from earlier examples of foreign fighters4), for example, are often thought of as examples of “new” terrorism (where initial engagement seems to actively involve social media of various kinds), who after experience of combat may become “old” terrorists as they become part of some kind of command structure. The processes that facilitate these transitions are clearly important points for preventative intervention. There are some grounds for supposing that similar processes are beginning to influence the emergence of complex criminal conspiracies.

All terrorist groups (as opposed to revolutionary movement, or guerrilla armies) are small. They may be part of some larger whole, but their (necessarily) secretive qualities ensure they are effectively small and limited in size. A difference that might be suggested is that new terrorism in the sense used here is aggregated “lone wolf” rather than an organized whole, and the collectivity of “newness” is characterized by global microstructures which are mediated by scopic media (as noted above, scopic media is where representation becomes independent of what is being represented. In this context it is primarily visual in character, and not achieved through written material, although sound and song presumably might be included). New terrorism, like many forms of criminal activity, expresses itself in both virtual and real life, but a central quality is that it is grounded in a sense of virtual microstructure.

The terrorist organization we refer to as Islamic State (IS) illustrates both “old” and “new” terrorism in the sense used here. There clearly is a strong sense in which the penetration of Islamic State into the West is as a “new” terrorist organization in its use of the Internet (and essentially through scopic media), and it has a strong but informal and distributed support base that articulates itself through, for example, social media – a clear example of a complex global microstructure. In this sense, the presence of IS in the West is essentially a virtual presence, but one that leaks into real life as supporters migrate from online activity, to offline activism that at the worst culminates either in attempts to proselytize, travel to become a fighter or the commission of a local terrorist act. However, in its contrasting “old” terrorist organizational state it has a very effective and strong non-virtual presence, in that it controls effectively an army, fights battles, commits terrorism atrocities and in addition has many of the qualities of a state.

This short analysis of terrorism helps to point up a disturbing potential future that goes beyond the problems of terrorism. The Europol Serious and Organised Crime Threat Assessment Report 2013 noted the potential of “unintended consequences of technology in terms of enabling or facilitating unforeseen criminal consequences”. In this paper, I suggest that what we will see develop is a working out of those unexpected consequences in terms of criminality, through the emergence of highly adaptive global microstructures. Commonalities between different kinds of online criminal engagement between terrorist and criminal offenders are already apparent, presumably reflecting the kinds of dynamic processes suggested here (Quayle & Taylor, 2015). Examination of seized hard drives of terrorist offenders, for example, show parallels, in terms of processes of engagement with the Internet, with another Internet-based criminal activity, the trade in child pornography.
To illustrate this theme further, a computer hard drive of a convicted terrorist examined by the author contained around 3000.jpg images – about a fifth scenes of emotive/Islamic material, and about three-quarters images of warfare, guns, and so on; the rest were a mixture of maps, pictures of leaders, notable figures, etc. Most were carefully catalogued into folders for geographical area, type, with sub-folders and so on (for example, in a folder “Weaponry”, there were sub-folders “Aircraft”, “Atomic bombs”, “bomb-guns”, “missiles-rockets”, “ships”, “swords”, “tanks-apc”, “weapons”). They were acquired over a period of about five years. Of the total four were singled out for the indictment, showing pictures of children wearing suicide vests, and suchlike. This offender also had 641 documents on his hard drive – some short Islamic judgements or views, some longer, and a small amount of academic material. Of particular interest were texts in Arabic – the computer owner spoke no Arabic, which raises the question of why these files were originally collected, retained, and organized. There was also some personal material (recipes for example, and personal details, pictures and so on).

This organizational pattern of material is like that found on seized drives of child pornography offenders (although content differs of course). The similarities reflect both the processes of engagement with the Internet (process and content) and the structure of an operating system’s management of computer files. For example, the large collection of emotionally charged images which show evidence of organization (by being placed in an organizational structure, which implies time, effort, and cognitive engagement) are strikingly similar, which suggests the significance of emotional valence as a facilitating factor (Quayle & Taylor, 2015); the presence of Arabic material also suggests acquisition of material as a token, rather than as a meaningful document.

Child pornography offenders are clearly different from terrorists in terms of intention and motivation, but I suggest there are similarities in terms of the way the Internet is used which reflects Internet processes, and also the qualities rather than the nature of content (a preponderance of essentially image-related material). A further important similarity in both, of course, is the danger to society posed by migration from online to offline activity, raising the issue of whether or not there are similar processes at work that might drive this migration. The significance of exploring these issues, of which examining hard drives is an example, is that what is accessed is a reflection of an individual’s behaviour on the Internet, and offers one way of accessing the process of Internet engagement – in the case of hard drive content, it constitutes a form of behavioural recording known as permanent product (Kelly, 1976). The merger of qualities of criminality suggested above not soley expressed in terms of images (although the significance of scopic mechanisms cannot be underestimated), mediated by Internet processes, merits further analysis, and may have profound operational implications.

Other similarities related to the potential for offending and risk related to Internet use can be drawn. Social networking, for example, is a ubiquitous form of communication for young (and not so young) people. It enables rapid and multiple threads of contact between people without limitation of geography or cost, sometimes with beneficial results, but sometimes contributing to enhanced risk of harm. As noted earlier, the qualities of social networking platforms shape, or afford, certain practices and usage, which the user also modifies through the way in which settings are used, and the use of, for example, multiple accounts (Livingstone, Haddon, Gøtzig, & Ólafsson, 2011). This creates a complex dynamic environment, in which both recipient and originator of communication reciprocally participate. The way such platforms are used relates to risk of harm (Quayle & Taylor, 2015; Staksrud, Ólafsson, & Livingstone, 2013), with some activities (enhanced public profile, large number of contacts, showing identifying information) particularly
enhancing risk of harm in children, including soliciting contacts by third parties. Indeed, Staksrund et al. (2013) conclude by noting that how social networking sites are used probably matters more in terms of experience of risk of harm than whether or not social networking sites are used. As an example in a more specific arena, enhanced risky sexual behaviour amongst young people may also associated with enhanced online activity (Rice et al., 2010).

The way that social networking sites affect behaviour can usefully be conceptualized in terms of the affordances and collaborative learning (Ryberg & Christiansen, 2008) such sites offer. There is growing evidence of the utility of this approach in understanding online sexual predation using the Internet (Quayle, Allegro, Hutton, Sheath, & Lööf, 2014). This study suggested that

the Internet was used to create a private space within which to engage in purposive, sexual behavior with young people. This engagement was for all an aid to fantasy, and for some was a precursor to an offline sexual assault. The opportunities afforded by Internet platforms not only allowed access to young people but facilitated the rapid acquisition of expertise. (Quayle et al., 2014, p. 368)

There is no reason to suppose that terrorist-related predation on young people operates in any different way, substituting perhaps a sense of “pop-up” ideology for the role of sexual fantasy.

The notion of “pop-up” ideology is relevant, because it implies not a complex carefully worked out political and philosophical structure, but an easily assimilated narrative, suited to the capacities and affordances offered by social networking. We know that complex ideological understanding does not characterize most terrorist’s engagement (McCauley & Moskalenko, 2011), but rather ideas of justice and empathy (Moskalenko & McCauley, 2011), notions that carry emotional valence that does not demand great intellectual engagement.

The essence of the argument presented here is that problematic behaviour on the Internet, whatever form it might take, is at least sustained, if not created, by the way we interact with the Internet. A critical element of this may be what has been termed “online disinhibition” (Suler, 2004), and the way that might interact with heightened emotional states. Online disinhibition refers to the way “some people self-disclose or act out more frequently or intensely than they would in person” (Suler, 2004, p. 321). Suler suggests that there are six factors that interact with each other to create this effect: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimization of authority. Blakeney, Findley, Self, Ingram, and Garrett (2010) suggest that high-level use of Facebook/MySpace is associated with high levels of disinhibition. We also know that self-disclosure occurs more rapidly in Internet-mediated communication than offline (Rossen, 1999), and the potential for psychological vulnerability all of this implies offers one means of understanding how Internet engagement and interaction can lead to behaviour that would be unlikely offline. Our experience of the Internet is essentially as a “performative” dynamic medium, and as such it may be that we need to revise our sense of concepts like risk (Montelius & Nygren, 2014).

Does this analysis support the notion that the Internet has criminogenic qualities? This may be a reasonable assertion in two senses. Firstly the distributed nature of the Internet, and the lack of control over content, is a factor in increased availability of illegal or undesirable material. Secondly, the way distributed complex global microsystems develop is effectively to increase opportunity for access to that content, some of which will be illegal. Associated with this, criminal conspiracies (within which I include terrorism) can...
deliberately and intentionally use both content and opportunity to engage with, and draw in, otherwise uncommitted people. Although I am unaware of empirical verification, it seems reasonable to suggest a symbiotic relationship will develop between these two factors, thus drawing participants more and more into engagement.

Disclosure statement
No potential conflict of interest was reported by the author.

Notes
1. An affordance is a quality of an object that enables or facilitates action (Gibson, 1977). For a discussion of how the concept of affordance relates to criminal activity and terrorism see Taylor and Currie (2012).
2. For an extended discussion of evolutionary influences on terrorism, see Taylor, Roach, and Pease (2015).
3. Scopic media are screen-based technologies of observation and projection that render distant and invisible phenomena situationally present, unfold remote spaces and information worlds, and shift the boundaries between situation/system and the environment. Scopic media mechanisms point away from relational connectivity, indicating global microstructures more than simply networks. In a networked digital environment, the morphology of the Internet is itself a significant factor. “Scopic systems acts as centering and mediating device through which things become assembled and from which they are projected forward.” They give concreteness and substance to temporal coordination, which acts as a mirroring device and also contextualizing mechanism.
4. See Jenson (2015) for an account of earlier forms of foreign fighters.

References


